FI0001053858

(12) PATENTTIJULKAISU
PATENTSKRIFT

(10) FI 105385 B

(45) Patentti myönnetty - Patent beviljats 31.07.2000

(51) Kv.lk.7 - Int.kl.7
H04Q 7/38, H04L 9/00

(21) Patenttihakemus - Patentansökning 974133

(22) Hakemispäivä - Ansökningsdag 04.11.1997

(24) Alkupäiva - Löpdag 04.11.1997

(41) Tullut julkiseksi - Blivit offentlig 05.05.1999

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

1 •Nokia Networks Oy, Helsinki, Keilalahdentie 4, 02150 Espoo, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare

1 •Virtanen, Sami, Sinipiianpolku 11 as. 14, 02100 Espoo, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Patenttitoimisto Compatent Oy
Pitkänsillanranta 3 B, 00530 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

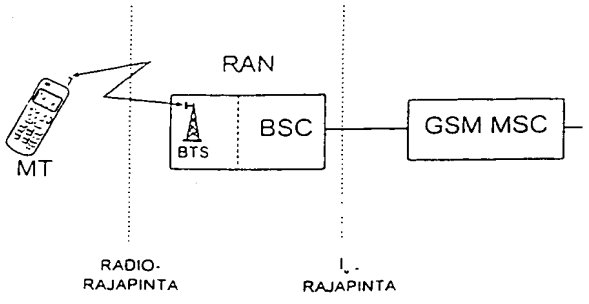
Menetelmä yhteyden salauksen asettamiseksi radiojärjestelmässä
Förfarande för fastställande av chiffrering av en förbindelse i ett radiosystem

(56) Viitejulkaisut - Anförda publikationer

—

(57) Tiivistelmä - Sammandrag

Eri radiojärjestelmien yhdistelmäjärjestelmissä, esimerkiksi IMT-2000 -järjestelmän radioverkon (RAN) ja GSM-järjestelmän runkoverkon (MSC) yhdistelmäjärjestelmässä, ongelmana on salausasetusten välittäminen järjestelmän elementiltä toisille. Esillä olevaa keksintö koskee menetelmää yhteyden salauksen asettamiseksi tällaisessa yhdistelmäjärjestelmässä, jossa keskuksen (MSC) ja radioverkon tukiaseman (BTS) salausasetusten käsittely suoritetaan eri protokollatasoilla kuin päätelaitteiden (MT) salausasetusten käsittely. Menetelmässä salaus järjestetään tukiaseman (BTS) ja päätelaitteen (MT) väliselle yhteydelle ja siinä lähetetään salausasetus keskukselta (MSC) radioverkon (RAN) ohjainyksikölle (BSC). Menetelmälle on keksinnön mukaisesti tunnusomaista, että siinä välitetään ohjainyksiköltä (BSC) tukiasemalle (BTS) salausasetus, joka on vain tukiaseman käyttöön, ja välitetään salausasetus ohjainyksiköltä (BSC) päätelaitteelle (MT) tukiaseman (BTS) kannalta läpinäkyvästi.



Vid system som kombinerats av olika radiosystem, t.ex. ett system som kombinerats av ett radionät (RAN) enligt IMT-2000 systemet och ett basnät (MSC) enligt GSM systemet utgör förmedlandet av krypteringsinställningarna från ett element i systemet till ett annat ett problem. Föreliggande uppfinning avser ett förfarande för inställning av krypteringen för en förbindelse i ett sådant kombinerat system där centralens (MSC) och radionätets basstations (BTS) behandling av krypteringsinställningarna utförs på olika protokollnivåer än terminalernas (MT) behandling av krypteringsinställningarna. Vid förfarandet anordnas krypteringen i förbindelsen mellan basstationen (BTS) och terminalen (MT) och där sänds krypteringsinställningen från centralen (MSC) till radionätets (RAN) styrenhet (BSC). Förfarandet kännetecknas enligt uppfinningen av att där förmedlas från styrenheten (BSC) till basstationen (BTS) en krypteringsinställning endast för basstationens användning, och krypteringsinställningen förmedlas från styrenheten (BSC) till terminalen (MT) ur basstationens (BTS) synvinkel transparent.

Menetelmä yhteyden salauksen asettamiseksi radiojärjestelmässä

Keksinnön ala

Keksintö koskee menetelmää yhteyden salauksen asettamiseksi radiojärjestelmässä, joka käsittää useita päätelaitteita, ainakin yhden keskuksen ja siihen yhteydessä olevan ainakin yhden radioverkkoyksikön, joka edelleen käsittää ainakin yhden ohjainyksikön ja sen ohjauksessa olevan ainakin yhden tukiaseman. Radiojärjestelmässä keskuksen ja tukiaseman salausasetusten käsittely suoritetaan eri protokollatasoilla kuin päätelaitteiden salausasetusten käsittely.

Tekniikan tausta

Yleisiltä radiojärjestelmiltä edellytetään nykyään keskinäistä yhteensopivuutta. Toisinaan tavoitteena on myös eri järjestelmistä olevien yksiköiden yhdistäminen toimivaksi kokonaisuudeksi, esimerkiksi tukiasemajärjestelmän yhteiskäyttö eri radiojärjestelmien runkoverkoissa. Kuvio 1 esittää erään tällaisen usean radiojärjestelmän yhdistelmän, jossa radioverkko RAN (Radio Access Network) on kytkettynä eri järjestelmien runkoverkkoihin, kuviossa GSM (Global System for Mobile communications), IMT-2000 (International Mobile Telecommunication), GPRS (General Packet Radio Service) ja ISDN (Integrated Services Digital Network) runkoverkkoihin. Tällainen radioverkko RAN on suunniteltu toteutettavaksi esimerkiksi tulevaisuuden IMT-2000 -järjestelmään. RAN-verkon avulla muodostetaan radioyhteys usean runkoverkon tilaajille, joten sitä kutsutaan myös yleiskäyttöiseksi radioverkoksi GRAN (Generic Radio Access Network). Kukin runkoverkko tarjoaa palvelut omille tilaajilleen. Päätelaite MT (Mobile Terminal) on siis radioteitse kytkeytyneenä radiorajapinnan yli johonkin radioverkon RAN tukiasemaan BTS, jonka kautta yhteys välitetään radioverkosta RAN päätelaitteen MT koti-runkoverkkoon I_u-rajapinnan yli. I_u-rajapinnalla tarkoitetaan avointa rajapintaa, jonka avulla eri järjestelmien RAN ja runkoverkko CN (Core Network) voidaan kytkeä yhteen. Runkoverkolla tarkoitetaan matkapuhelinkeskusta MSC (Mobile Services Switching Centre) ja verkon muita yksiköitä, kuten esimerkiksi vierailijarekisteri VLR (Visitor Location Register), kotirekisteri HLR (Home Location Register), jne. järjestelmästä riippuen. I_u on esitetty käsittävän kerroksen 3 BN-protokollan (Bearer Negotiation) ja sen alemmat fyysisen välityksen kerrokset (transmission). Runkoverkko voi myös

koostua erillisestä paketti palvelusolmuista kuten GSM:n GPRS (General Packet Radio Service), SGSN (Serving GPRS Support Node) ja GGSN (Gateway GPRS Support Node).

Kuviossa 2 on tarkemmin esitetty GSM-runkoverkon liittyminen radioverkkoon RAN. Radioverkko RAN koostuu ainakin yhdestä tukiasemaohjaimesta BSC (Base Station Controller) ja sen alaisuudessa olevista tukiasemista BTS. GSM-verkon toiminnasta poiketen IMT-2000 -järjestelmän RAN-verkon ja päätelaitteen MT välinen signalointi on usein tukiasemalle BTS läpinäkyvää. Tukiasemaohjaimen BSC ja päätelaitteen MT välisessä signaloinnissa toistimena toimivan tukiaseman BTS rakenne on siten pelkistetympi kuin perinteisissä matkaviestinjärjestelmissä. Tukiasemaohjain BSC reitittää tukiaseman BTS kautta saapuneet päätelaitteen MT viestit GSM-järjestelmän matkapuhelinkeskukselle MSC ja toisin päin.

Ongelmana IMT-2000 -järjestelmän radioverkon RAN ja esimerkiksi GSM-järjestelmän runkoverkon yhdistämisessä on salauksen järjestäminen yhteyksille. IMT-2000 -järjestelmässä salaus on toteutettu päätelaitteen MT ja runkoverkon keskuksen MSC välille, jolloin liikennöinti on radioverkon RAN kannalta läpinäkyvää. GSM-järjestelmässä salaus on toteutettu ilmarajapinnalle matkaviestimen MS ja tukiaseman BTS välille. Seuraavassa yhdistelmäjärjestelmästä aiheutuvaa ongelmaa on selostettu tarkemmin kuvioiden 3 - 6 valossa.

Kuviossa 3 on esitetty GSM-järjestelmäkokonaisuuden yhteyden teoreettinen kerroskuvaus, jossa toistensa kanssa yhteydessä olevien yksiköiden samannimiset protokollat viestivät keskenään. Salaukseen osallistumattomat fyysisen välityksen kerrokset 1 ja 2 on havainnollisuuden vuoksi esitetty katkoviivoilla. Kuviossa yhtenäisellä viivalla esitetyt laatikot kuuluvat kerrokseen 3. Kuviossa esitetyistä protokollista CC (Call Control) suorittaa puhelun ohjausta ja MM (Mobility Management) matkaviestimen MS sijainnin hallintaa. GSM-järjestelmässä nämä protokollat eivät osallistu yhteyden salauksen toteuttamiseen.

Kuviossa 4 on esitetty GSM-järjestelmän salauksen asettaminen signalointikaaviona. Kuvioon 4 on myös merkitty kuvion 3 protokollalaatikoiden osallistuminen salauksen asetukseen. Matkapuhelinkeskus MSC lähettää BSSAP-protokollalla salauksen aloituskäskyn 41 CIPHERING_MODE_COMMAND tukiasemaohjaimen BSC BSSAP-protokollalle. BSSAP-protokolla (BSS Application Part) vastaa BN-protokollaa. Tukiasema-

ohjaimen BSC sisäisesti aloituskäsky välitetään sanomassa 42 BSSAP-protokollalta BTSM-protokollalle (BTS Management), joka kykenee viestimään tukiaseman BTS vastaavan protokollan kanssa. Tukiasemaohjaimen BSC BTSM-protokolla välittää siis salauskäskyn tukiaseman BTSM-protokollalle sanomassa 44 ENCRYPTION_COMMAND, joka sisältää matkaviestimelle MS välitettäväksi tarkoitetun RR-protokollan (Radio Resource management) CIPHERING_MODE_COMMAND-sanoman. Tukiaseman BTS sisäisesti salauskäsky välitetään BTSM-protokollalta sanomassa 45 RR'-protokollalle, joka on RR-protokollan osa ja pystyy siten viestimään matkaviestimen MS RR-protokollan kanssa. Tukiaseman BTS RR'-protokolla välittää sanoman 44 sisällä toimitetun CIPHERING_MODE_COMMAND-sanoman matkaviestimen MS RR-protokollalle (sanoma 46). Matkaviestimen MS RR-protokolla kuittaa salausasetuksen lähettämällä tukiasemaohjaimen BSC RR-protokollalle kuittaussanoman 47 CIPHERING_MODE_COMPLETE. Tukiasemaohjaimen BSC sisäisesti tämä kuittaus välitetään RR-protokollalta BSSAP-protokollalle (sanoma 48), joka edelleen välittää kuittaussanoman matkapuhelinkeskuksen BSSAP-protokollalle sanomassa 49 CIPHERING_MODE_COMPLETE. Matkaviestimen MS RR-protokolla ja tukiaseman BTS RR'-protokolla välittävät salausparametrit ja salauksen käynnistyskäskyn yksiköiden sisäisesti alemmille fyysisen yhteyden kerroksille, jotka suorittavat lähetyspäässä salausta ja vastaanottopäässä salauksen purkua ylempien protokollien signaaleille.

Kuviossa 5 on esitetty kuviota 3 vastaava yhteyden teoreettinen kerroskuvaus IMT-2000 -järjestelmäkokonaisuuden tapauksessa. Jälleen salaukseen osallistumattomat fyysisen välityksen kerrokset 1 ja 2 on merkitty kuvioon katkoviivoin. Kerrokset 1 ja 2 voivat olla esimerkiksi ATM-protokollalla toteutetut. IMT-2000 -järjestelmän CC-protokolla suorittaa puhelun ohjausta ja MM-protokolla päätelaitteen MT sijainnin hallinnan lisäksi alustaa yhteyden salauksen. TAC-protokolla (Terminal Association Control) muodostaa yhteyden verkon ja päätelaitteen MT välille.

Kuviossa 6 on esitetty IMT-2000 -järjestelmän salauksen alustus signalointikaaviona. Salauksen alustus suoritetaan MM-T-protokollalla (Mobility Management - Terminal) radioverkon RAN kannalta läpinäkyvästi. Keskus MSC lähettää MM-T-protokollalla päätelaitteelle MT salauksen alustussanoman 61 MOBILITY_FACILITY_(START_CIPHERING: INVOKE). Radioverkko RAN välittää viestin suoraan päätelaitteelle MT, joka kuittaa sala-

uksen alustuksen sanomalla 62 MOBILITY_FACILITY (START_CIPHERING: RETURN_RESULT). Myös sanoma 62 välitetään keskukselle MSC radioverkon RAN kannalta läpinäkyvästi. Radioverkon RAN tukiasema BTS ja tukiasemaohjain BSC, joiden läpi sanomat kulkevat, eivät siis osallistu salaukseen eivätkä tiedä salauksesta. Yhteyden salaus toteutetaan alustuksen jälkeen keskuksen MSC ja päätelaitteen MT välille.

Ongelmana on siis kuviossa 2 esitetyssä järjestelmäkokoonpanossa se, että matkapuhelinkeskus ei tue salausasetusten suoraa välitystä päätelaitteelle radioverkon RAN yli läpinäkyvästi. Edelleen ongelmana on, että radioverkon RAN tukiasemalla BTS ei ole salausasetuksia käsittelevää protokollaa, joka kykenisi viestimään päätelaitteen vastaavan protokollan kanssa, joten salauksen alustusta ei pystytä suorittamaan tukiaseman ja päätelaitteen välillä. Tällöin kuvion 2 mukaisessa järjestelmäkokoonpanossa ei voida tunnetun tekniikan perusteella järjestää yhteydelle salausta.

Keksinnön lyhyt yhteenveto

Tämän keksinnön tarkoituksena on toteuttaa salaus radiorajapinnalle radiojärjestelmäkokoonpanossa, jossa tukiaseman salausasetuksia käsittelevä protokolla ei kykene viestimään päätelaitteen vastaavan protokollan kanssa.

Tämä uudentyyppinen salauksen asettaminen saavutetaan keksinnönmukaisella menetelmällä, jolle on tunnusomaista se, mitä on sanottu itsenäisessä patenttivaatimuksessa 1. Keksinnön erityisiä suoritusmuotoja on esitetty epäitsenäisissä patenttivaatimuksissa.

Keksintö perustuu siihen ajatukseen, että radioverkon ohjainyksikkö toimittaa salauksen alustusasetukset toisistaan riippumattomasti tukiasemalle ja päätelaitteelle. Ohjainyksiköltä välitetään siis tukiasemalle sen tarvitsemat salauksen alustusasetukset ja toisaalta päätelaitteelle sen tarvitsemat salauksen alustusasetukset tukiaseman kannalta läpinäkyvästi.

Tällaisen salauksen asettamisen etuna on se, että salaus pystytään järjestämään radiorajapinnan yli viestivien yksiköiden välille silloinkin, kun yksiköt eivät kykene viestimään salauksen alustusasetuksia keskenään, esimerkiksi GSM-runkoverkon ja IMT-2000 -järjestelmän radioverkon yhdistelmän tapauksessa.

Kuvioluettelo

Keksintöä selostetaan nyt lähemmin edullisen suoritusmuodon yhteydessä viitaten kuvioiden 2, 5 ja 7 mukaisiin esimerkkeihin oheisissa piirustuksissa, joissa:

kuvio 1 esittää radioverkon yhteiskäyttöön perustuvan radiojärjestelmän lohkokaaviona;

kuvio 2 esittää kuvion 1 radioverkon liittymisen GSM-runkoverkkoon;

kuvio 3 esittää keksinnön kannalta oleelliset GSM-järjestelmän yhteyden protokollat kerroskuvantona;

kuvio 4 esittää GSM-järjestelmän salauksen asettamisen signalointikaaviona;

kuvio 5 esittää keksinnön kannalta oleelliset IMT-2000 -järjestelmän yhteyden protokollat kerroskuvantona;

kuvio 6 esittää IMT-2000 -järjestelmän salauksen alustuksen signalointikaaviona; ja

kuvio 7 esittää keksinnön mukaisen salauksen asettamisen signalointikaaviona.

Keksinnön yksityiskohtainen selostus

Esillä olevaa keksintöä voidaan soveltaa minkä tahansa radiojärjestelmien yhdistelmän yhteydessä. Jäljempänä keksintöä on lähemmin selostettu esimerkinomaisesti etupäässä digitaalisen GSM-matkaviestinjärjestelmän runkoverkon ja IMT-2000 järjestelmän radioverkon yhdistelmän yhteydessä. Kuvioissa 1 ja 2 on esitetty aiemmin selostettu yksinkertaistettu radiojärjestelmien yhdistelmän rakenne. GSM-järjestelmän tarkemman kuvauksen osalta viitataan GSM-suosituksiin sekä kirjaan "The GSM System for Mobile Communications", M. Mouly & M. Pautet, Palaiseau, France, 1992, ISBN:2-9507190-0-7.

Seuraavassa keksintöä selostetaan tarkemmin keksinnön ensisijaisen suoritusmuodon valossa viitaten kuvioihin 2, 5 ja 7.

Kuvio 2 esittää aiemmin selostetun esimerkin radiojärjestelmäyhdistelmästä, jossa GSM-järjestelmän runkoverkko on yhteydessä radioverkon RAN kanssa. Päätelaite MT on sovitettu viestimään radioverkon RAN välityksellä GSM-runkoverkon kanssa siten, että kuviossa 5 esitetty päätelaitteen protokollapino koostuu GSM-järjestelmän MM- ja CC-protokollista ja

muilta osin radioverkon RAN edellyttämistä protokollista; kuvion 5 tapauksessa IMT-2000 -järjestelmän protokollista. Radioverkon RAN protokollarakenteessa salausasetuksia voidaan tarvittaessa käsitellä RBC- (Radio Bearer Control) ja BC-protokollatasoilla (Bearer Control) ja päätelaitteessa MT RBC-protokollatasolla.

Kuvio 7 esittää signalointikaaviona keksinnön mukaisen salauksen asettamisen kuvion 5 mukaisilla protokollatasoilla. Salauksen asettamisen aluksi matkapuhelinkeskus MSC lähettää radioverkolle RAN käskysanoman salauksen alustamiseksi (sanoma 71 CIPHERING_MODE_COMMAND). Sanoma 71 lähetetään GSM matkapuhelinkeskuksen MSC esimerkiksi BN-protokollalla, joka on I_u-rajapinnan kerroksen 3 protokolla. Tukiasemaohjaimen BSC BN-protokolla vastaanottaa tämän käskysanoman ja välittää sen tukiasemaohjaimen sisäisesti salausasetuksia käsittelevälle RBC-protokollalle (sanoma 72). Seuraavaksi tukiasemaohjain välittää salauksen aloituskäskyn kahdessa toisistaan riippumattomassa vaiheessa yhtäältä tukiasemalle BTS ja toisaalta päätelaitteelle MT. Kuviossa 7 on esitetty nämä kaksi vaihetta siten, että aluksi suoritetaan ensimmäisessä vaiheessa salauksen aloituskäskyn välitys tukiasemalle BTS ja sen jälkeen toisessa vaiheessa päätelaitteelle MT. Ensimmäisen ja toisen vaiheen signaloinnit voidaan myös suorittaa ainakin osittain samanaikaisesti tukiasemaohjaimen BSC prosessointikyvystä riippuen. Edellä määritetyt ensimmäinen ja toinen vaihe on merkitty kuvioon 7 roomalaisin numeroin I ja II.

Kuvion 7 esimerkkitapauksessa edellä määritetyssä ensimmäisessä vaiheessa tukiasemaohjain BSC välittää matkapuhelinkeskukselta MSC saamansa käskysanoman esillä olevan keksinnön mukaisesti RBC-protokollalta edelleen toiselle salausasetuksia käsittelevälle BC-protokollalle (sanoma 73). Tukiasemaohjaimen BC-protokolla lähettää tukiaseman BTS vastaavalle protokollalle salauskäskyn (sanoma 74 ENCRYPTION_COMMAND), jonka tukiasema BTS kuittaa sanomalla 75 ENCRYPTION_COMPLETE. Tukiasemaohjaimen BSC ja tukiaseman BTS väliset BC-protokollan sanomat 74 ja 75 välitetään siirtoyhteydellä esimerkiksi ATM-yhteyden AAL5-protokollalla. Tukiaseman BTS sisäisesti välitetään salausprosessista huolehtivalle fyysisen välityksen kerrokselle tieto salausasetuksista ja salauksen aloituksesta, jonka jälkeen fyysisen välityksen kerroksen protokolla aloittaa salauksen ja salauksen purkamisen annetuilla paramet-

reilla. Tukiasemaohjaimen BC-protokolla välittää tukiaseman kuittaussanoman edelleen tukiasemaohjaimen sisäisesti RBC-protokollalle (sanoma 76).

Kuvioon 7 määritetyssä toisessa vaiheessa tukiasemaohjaimen RBC-protokolla lähettää päätelaitteen MT vastaavalle protokollalle salauksen aloitussanoman 77 CIPHERING_COMMAND. Päätelaitteen MT sisäisesti RBC-protokolla välittää salausprosessista huolehtivalle fyysisen välityksen kerrokselle tiedon salausasetuksista ja salauksen aloituksesta, jonka jälkeen fyysisen välityksen kerroksen protokolla aloittaa salauksen ja salauksen purkamisen annetuilla parametreilla. Päätelaite MT kuittaa salauksen aloitussanoman lähettämällä tukiasemaohjaimen BSC RBC-protokollalle sanoman 78 CIPHERING_COMPLETE. Tukiasemaohjaimen BSC ja päätelaitteen MT väliset RBC-protokollan sanomat 77 ja 78 välitetään BSC:n ja BTS:n välillä esimerkiksi ATM:n AAL2-protokollalla.

Ensimmäisen ja toisen vaiheen suorituksen jälkeen tukiasemaohjaimen RBC-protokolla välittää tukiasemaohjaimen BSC sisäisesti BN-protokollalle kuittauksen salausasetusten perille toimituksesta (sanoma 79). Tukiasemaohjaimen BN-protokolla lähettää kuittaussanoman edelleen matkapuhelinkeskuksen MSC vastaavalle BN-protokollatasolle (sanoma 80 CIPHERING_MODE_COMPLETE).

Edellä selostetun salauksen asettamisen ansiosta tukiaseman BTS ja päätelaitteen MT välinen yhteys voidaan salata radiorajapinnan yli. Varsinainen radiorajapinnan yli toteutettava salaus on esimerkiksi vastaavanlainen kuin GSM-järjestelmässä.

Keksinnön toissijaisessa suoritusmuodossa käynnissä olevan yhteyden salausasetuksia muutetaan kesken yhteyden ja esimerkiksi kuviossa 7 esitettyä signalointia käytetään uusien salausasetusten välittämiseen fyysisestä salauksesta huolehtiville yksiköille. Seuraavassa keksinnön toissijaista suoritusmuotoa selostetaan tarkemmin viitaten kuvioon 7.

Keksinnön toissijaisessa suoritusmuodossa salauksen asetuksen sanomat 71 - 73 välitetään kuten edellä on keksinnön ensisijaisen suoritusmuodon yhteydessä selostettu. Edelleen keksinnön toissijaisen suoritusmuodon ensimmäisessä vaiheessa tukiasemaohjain BSC välittää tukiasemalle BTS esimerkiksi BC-protokollalla salausasetussanoman 74, jonka tukiasema BTS kuittaa sanomalla 75. Kuittaus välitetään tukiasemaohjaimen BSC sisäisesti sanomassa 76 kuten edellä ensisijaisen suoritusmuodon yhteydessä on selostettu. Tukiaseman BTS sisäisesti uudet salausasetukset ja

tieto salauksen muuttamisesta välitetään salausprosessista huolehtivalle fyysisen välityksen kerrokselle, joka uudet asetukset saatuaan jatkaa tukiaseman BTS ja päätelaitteen MT välisen yhteyden salaamista ja salauksen purkamista uusien asetusten mukaisesti, esimerkiksi vaihtaa käytettävää salausalgoritmia.

Keksinnön toissijaisen suoritusmuodon toisessa vaiheessa tukiasemaohjain BSC välittää päätelaitteelle MT tukiaseman kautta läpinäkyvästi esimerkiksi RBC-protokollalla salausasetussanoman 77. Mikäli salausasetussanoma 77 lähetetään radiorajapinnalla salattuna päätelaitteelle MT, käytetään sanoman salaukseen vanhoja salausasetuksia, esimerkiksi uudeksi muutettavaa salausalgoritmia. Päätelaitteen MT sisäisesti uudet salausasetukset ja tieto salauksen muuttamisesta välitetään salausprosessista huolehtivalle fyysisen välityksen kerrokselle, joka uudet asetukset saatuaan jatkaa päätelaitteen MT ja tukiaseman BTS välisen yhteyden salaamista ja salauksen purkamista uusien asetusten mukaisesti, esimerkiksi vaihtaa käytettävää salausalgoritmia. Päätelaite MT kuittaa uusien salausasetusten vastaanottamisen sanomalla 78. Jälleen mikäli kuittaussanoma 78 halutaan lähettää radiorajapinnalla salattuna, käytetään salaukseen uusia salausasetussanomassa 77 toimitettuja salausasetuksia, esimerkiksi uutta salausalgoritmia. Kuittaussanomat 79 ja 80 välitetään kuten ensisijaisen suoritusmuodon yhteydessä on selostettu.

Piirustukset ja niihin liittyvä selitys on tarkoitettu vain havainnollistamaan keksinnön ajatusta. Yksityiskohdiltaan voi keksinnön mukainen menetelmä vaihdella patenttivaatimusten puitteissa. Edellä selostetun esimerkin mukaiset sanomat ja protokollatasot on vain eräs toteutusvaihtoehto eikä keksintö siten rajoitu pelkästään näiden sanomien välitykseen tai esitettyihin protokollatasoihin. Vaikka keksintöä onkin edellä selitetty lähinnä IMT-2000 -järjestelmän radioverkon RAN ja GSM-runkoverkon yhdistelmän yhteydessä, voidaan menetelmää käyttää muunkinlaista radiojärjestelmää varten, erityisesti kun salausprosessiin osallistuvat yksiköt eivät kykene suoraan viestimään salausasetuksia toisilleen. Keksintö soveltuu käytettäväksi esimerkiksi IMT-2000 -järjestelmän radioverkon RAN tai vastaavan ja jonkin runkoverkon keskuksen yhdistelmänä muodostetussa yleisessä radiojärjestelmässä, jossa salausasetuksia ei välitetä keskukselta läpinäkyvästi radioverkon yli päätelaitteelle.

Patenttivaatimukset

1. Menetelmä yhteyden salauksen asettamiseksi radiojärjestelmässä, joka käsittää useita päätelaitteita (MT), ainakin yhden keskuksen (MSC) ja siihen yhteydessä olevan ainakin yhden radioverkkoyksikön (RAN), joka edelleen käsittää ainakin yhden ohjainyksikön (BSC) ja sen ohjauksessa olevan ainakin yhden tukiaseman (BTS), jossa radiojärjestelmässä keskuksen (MSC) ja tukiaseman (BTS) salausasetusten käsittely suoritetaan eri protokollatasoilla kuin päätelaitteiden (MT) salausasetusten käsittely, jossa menetelmässä

lähetetään salausasetus keskukselta (MSC) radioverkon (RAN) ohjainyksikölle (BSC) ja

salataan salausasetuksilla tukiaseman (BTS) ja päätelaitteen (MT) välinen yhteys,

tunnettu siitä, että menetelmässä

välitetään ohjainyksiköltä (BSC) tukiasemalle (BTS) salausasetus, joka on vain tukiaseman käyttöön, ja

välitetään salausasetus ohjainyksiköltä (BSC) päätelaitteelle (MT) tukiaseman (BTS) kannalta läpinäkyvästi.

2. Patenttivaatimuksen 1 mukainen menetelmä, tunnettu siitä, että

välitetään salausasetus ohjainyksiköltä (BSC) tukiasemalle (BTS) ensimmäisellä protokollalla ja

välitetään salausasetus ohjainyksiköltä (BSC) päätelaitteelle (MT) toisella protokollalla, joka on eri kuin ensimmäinen protokolla.

3. Patenttivaatimuksen 2 mukainen menetelmä, tunnettu siitä, että salausasetusten välittämiseksi

lähetetään ohjainyksiköltä (BSC) tukiasemalle (BTS) sanoma salausasetusten ilmoittamiseksi tukiasemalle (74),

lähetetään tukiasemalta (BTS) ohjainyksikölle (BSC) sanoma tukiaseman salausasetusten kuittaamiseksi (75),

lähetetään ohjainyksiköltä (BSC) päätelaitteelle (MT) sanoma salausasetusten ilmoittamiseksi päätelaitteelle (77), ja

lähetetään päätelaitteelta (MT) ohjainyksikölle (BSC) sanoma päätelaitteen salausasetusten kuittaamiseksi (78).

4. Patenttivaatimuksen 3 mukainen menetelmä, tunnettu siitä, että lisäksi välitetään tukiaseman salausasetusten kuittaussanoma (75) ohjainyksikön (BSC) sisäisesti protokollalta toiselle.

5. Patenttivaatimuksen 3 mukainen menetelmä, tunnettu siitä, että

salataan salausasetusten päätelaitteelle ilmoittamissanoma (77) vanhalla salausasetuksella ja

salataan salausasetusten kuittaussanoma päätelaitteelta (78) uudella salausasetuksella.

6. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, tunnettu siitä, että

välitetään salausasetus kesken liikennöintiyhteyden salauksen muuttamiseksi toiseksi.

Patentkrav

1. Förfarande för inställning av krypteringen av en förbindelse i ett radiosystem som omfattar flera terminaler (MT), åtminstone en central (MSC) och åtminstone en radionätsenhet (RAN) som står i förbindelse med denna, vilken vidare omfattar åtminstone en styrenhet (BSC) och en av denna styrd åtminstone en basstation (BTS), i vilket radiosystem behandlingen av centralens (MSC) och basstationens (BTS) krypteringsinställningar utförs på olika protokollnivåer än behandlingen av terminalernas (MT) krypteringsinställningar, vid vilket förfarande

en krypteringsinställning sändes från centralen (MSC) till radionätets (RAN) styrenhet (BSC), och

förbindelsen mellan basstationen (BTS) och terminalen (MT) krypteras med krypteringsinställningarna,

kännetecknat av att vid förvarandet

förmedlas från styrenheten (BSC) till basstationen (BTS) en krypteringsinställning endast för basstationens användning, och

förmedlas krypteringsinställningen från styrenheten (BSC) till terminalen (MT) ur basstationens (BTS) synvinkel transparent.

2. Förfarande enligt patentkrav 1, kännetecknat av att

krypteringsinställningen förmedlas från styrenheten (BSC) till basstationen (BTS) med ett första protokoll, och

krypteringsinställningen förmedlas från styrenheten (BSC) till terminalen (MT) med ett andra protokoll, som är ett annat än det första protokollet.

3. Förfarande enligt patentkrav 2, kännetecknat av att för förmedling av krypteringsinställningarna

sänds från styrenheten (BSC) till basstationen (BTS) ett meddelande för att meddela krypteringsinställningarna till basstationen (74),

sänds från basstationen (BTS) till styrenheten (BSC) ett meddelande för kvittering av basstationens krypteringsinställningar (75),

sänds från styrenheten (BSC) till terminalen (MT) ett meddelande för att meddela krypteringsinställningarna till terminalen (77), och

sänds från terminalen (MT) till styrenheten (BSC) ett meddelande för kvitteringav terminalens krypteringsinställningar (78).

4. Förfarande enligt patentkrav 3, kännetecknat av att dessutom förmedlas kvitteringsmeddelandet (75) för basstationens krypteringsinställningar internt i styrenheten (BSC) från ett protokoll till ett annat.

5. Förfarande enligt patentkrav 3, kännetecknat av att krypteringsinställningarnas budskaps meddelande (77) till terminalen krypteras med den gamla krypteringsinställningen, och krypteringsinställningarnas kvitteringsmeddelande från terminalen (78) krypteras med en ny krypteringsinställning.

6. Förfarande enligt patentkrav 1 eller 2, kännetecknat av att krypteringsinställningen förmedlas mitt under trafikförbindelsen för att ändra krypteringen.

Fig. 1

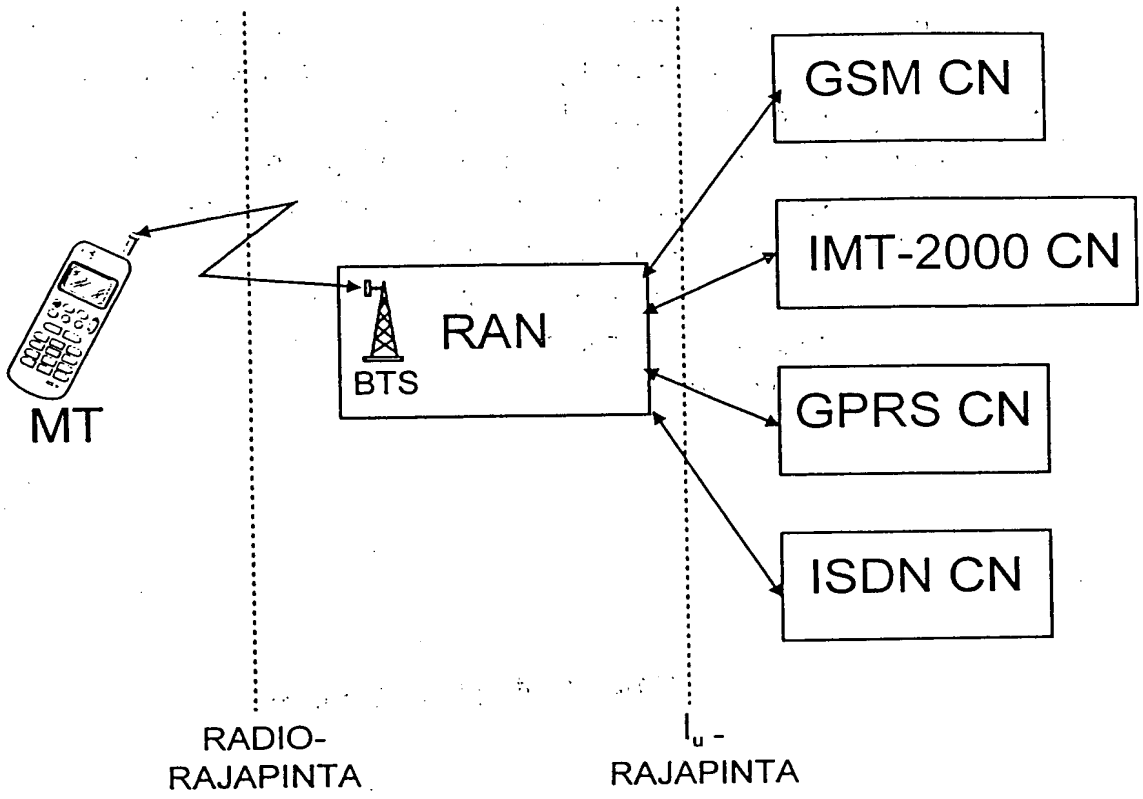

GSM CN
IMT-2000 CN
GPRS CN
ISDN CN
RAN
BTS
MT
RADIO-
RAJAPINTA
Iu -
RAJAPINTA

Fig. 2

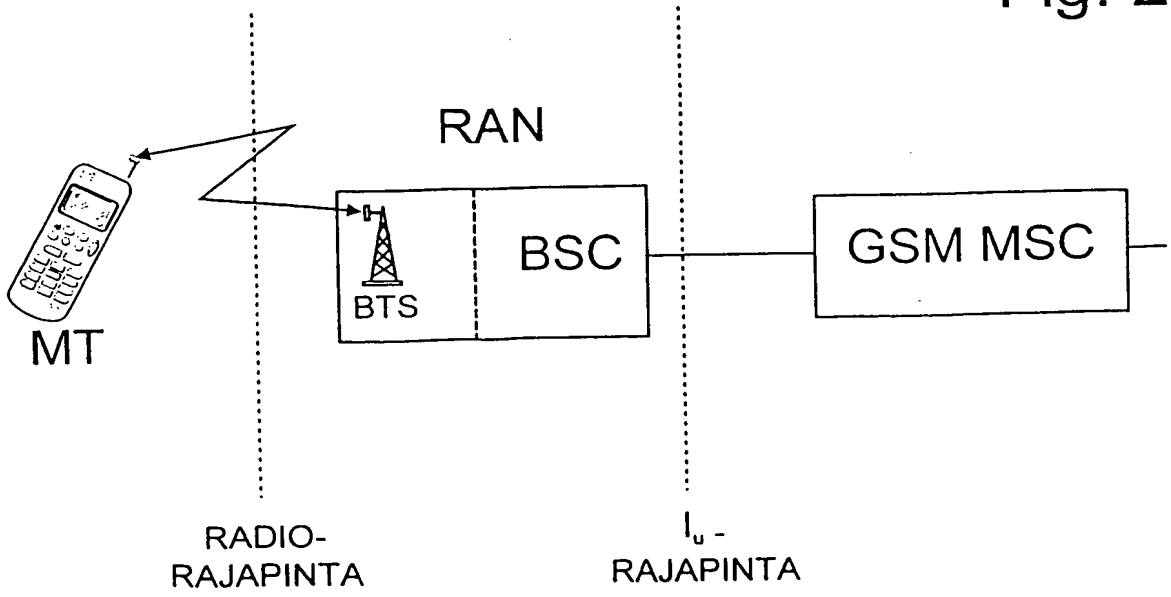

RAN
BSC
BTS
GSM MSC
MT
RADIO-
RAJAPINTA
Iu -
RAJAPINTA

Fig. 3

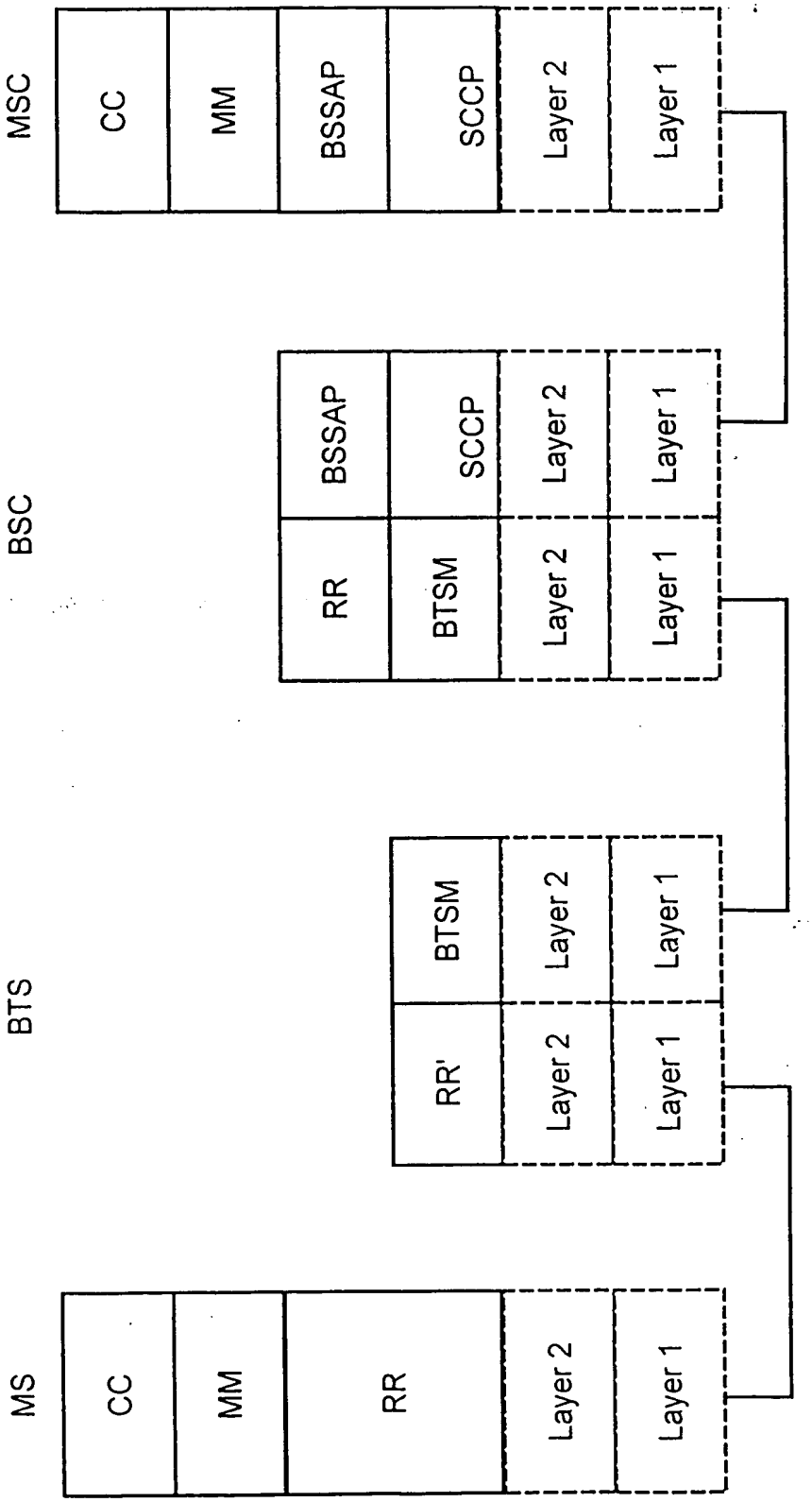

MSC
CC
MM
BSSAP
SCCP
Layer 2
Layer 1
BSC
RR
BTSM
BSSAP
SCCP
Layer 2
Layer 1
BTS
RR'
BTSM
Layer 2
Layer 1
MS
CC
MM
RR
Layer 2
Layer 1

Fig. 4

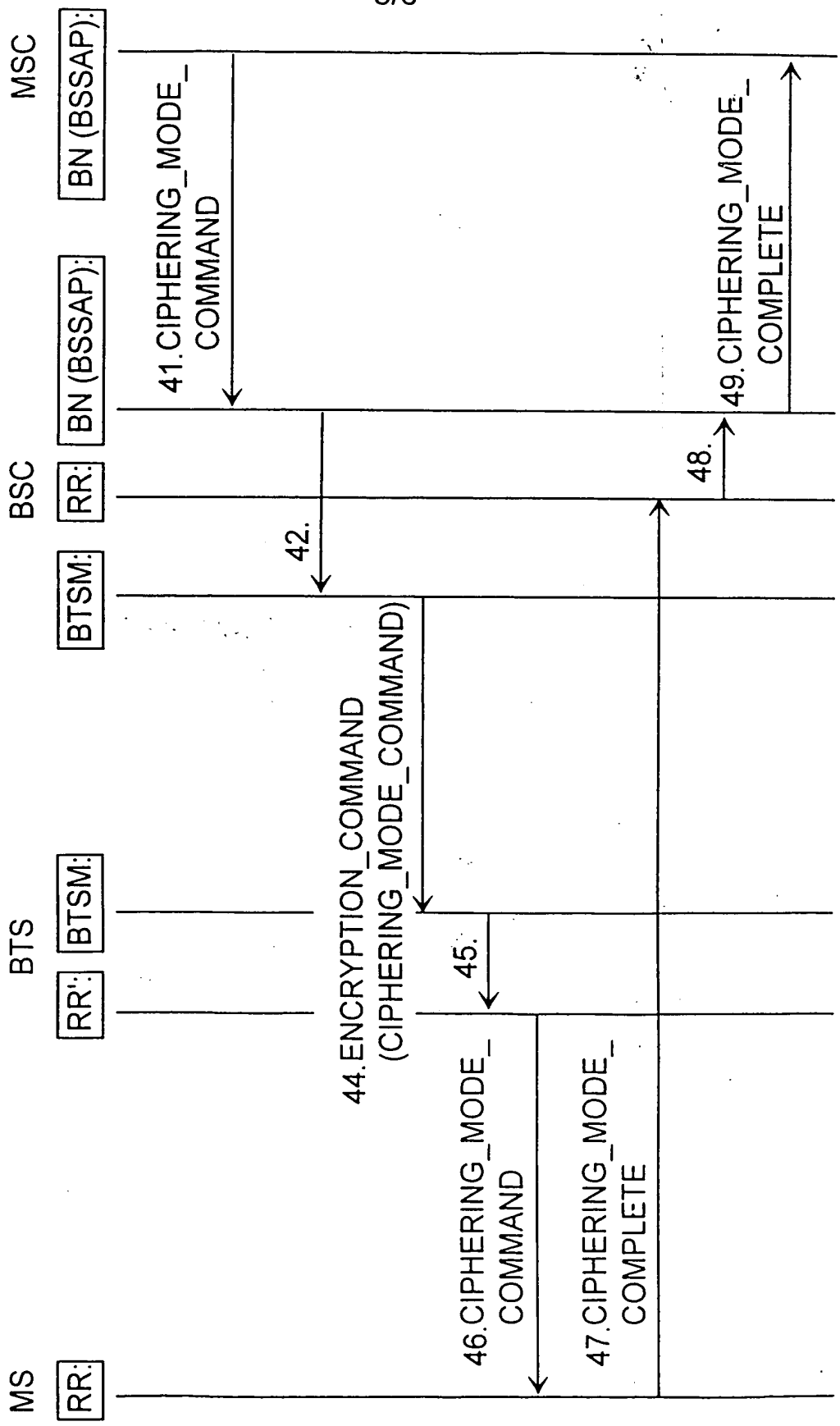

MSC
BN (BSSAP):
BSC
BN (BSSAP):
RR:
BTSM:
BTS
BTSM:
RR':
MS
RR:
41.CIPHERING_MODE_ COMMAND
42.
44.ENCRYPTION_COMMAND (CIPHERING_MODE_COMMAND)
45.
46.CIPHERING_MODE_ COMMAND
47.CIPHERING_MODE_ COMPLETE
48.
49.CIPHERING_MODE_ COMPLETE

Fig. 5

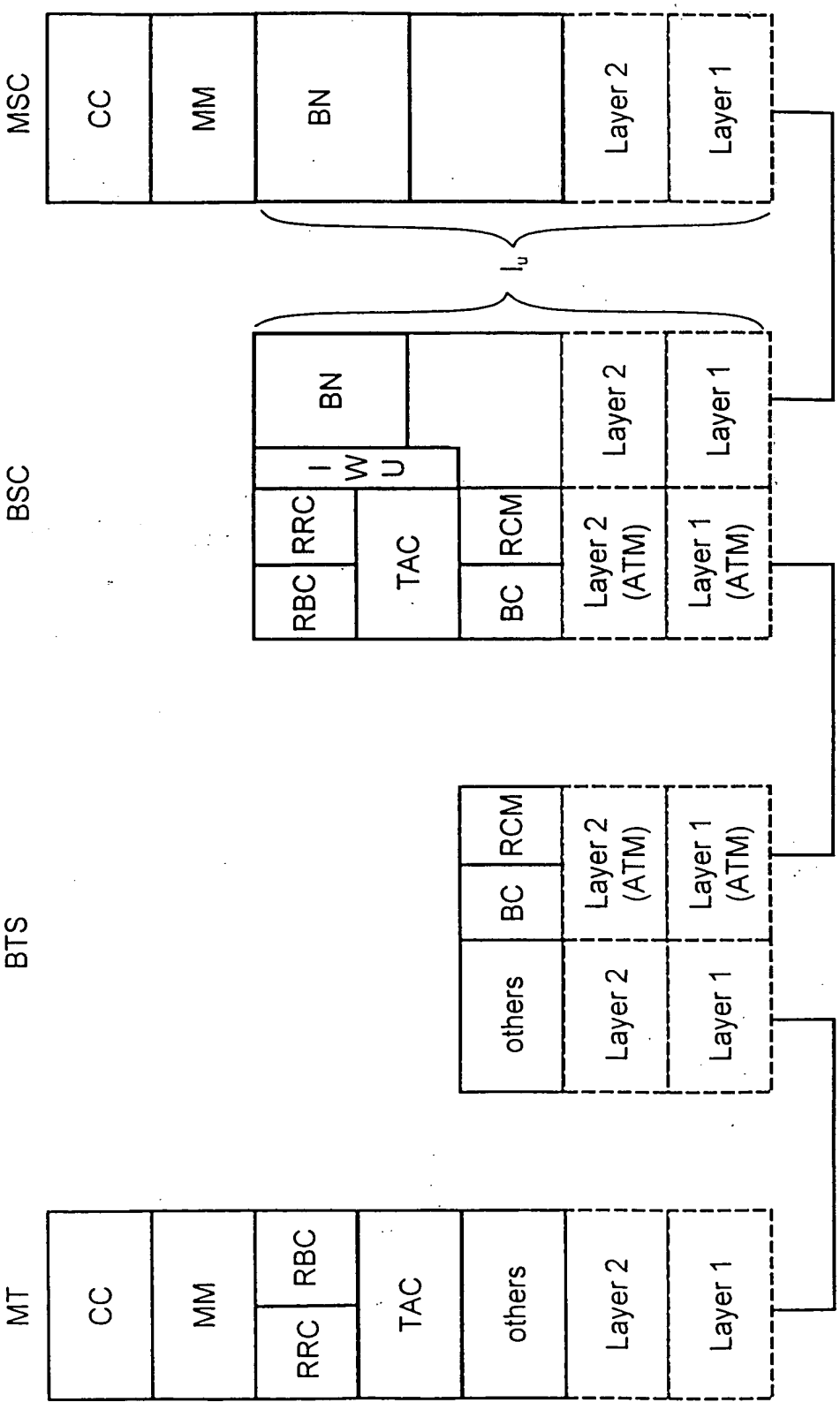

MSC
CC
MM
BN
Layer 2
Layer 1
I_u
BSC
BN
I
W
U
RRC
RBC
TAC
RCM
BC
Layer 2
Layer 1
Layer 2 (ATM)
Layer 1 (ATM)
BTS
others
Layer 2
Layer 1
BC
RCM
Layer 2 (ATM)
Layer 1 (ATM)
MT
CC
MM
RRC
RBC
TAC
others
Layer 2
Layer 1

Fig. 6

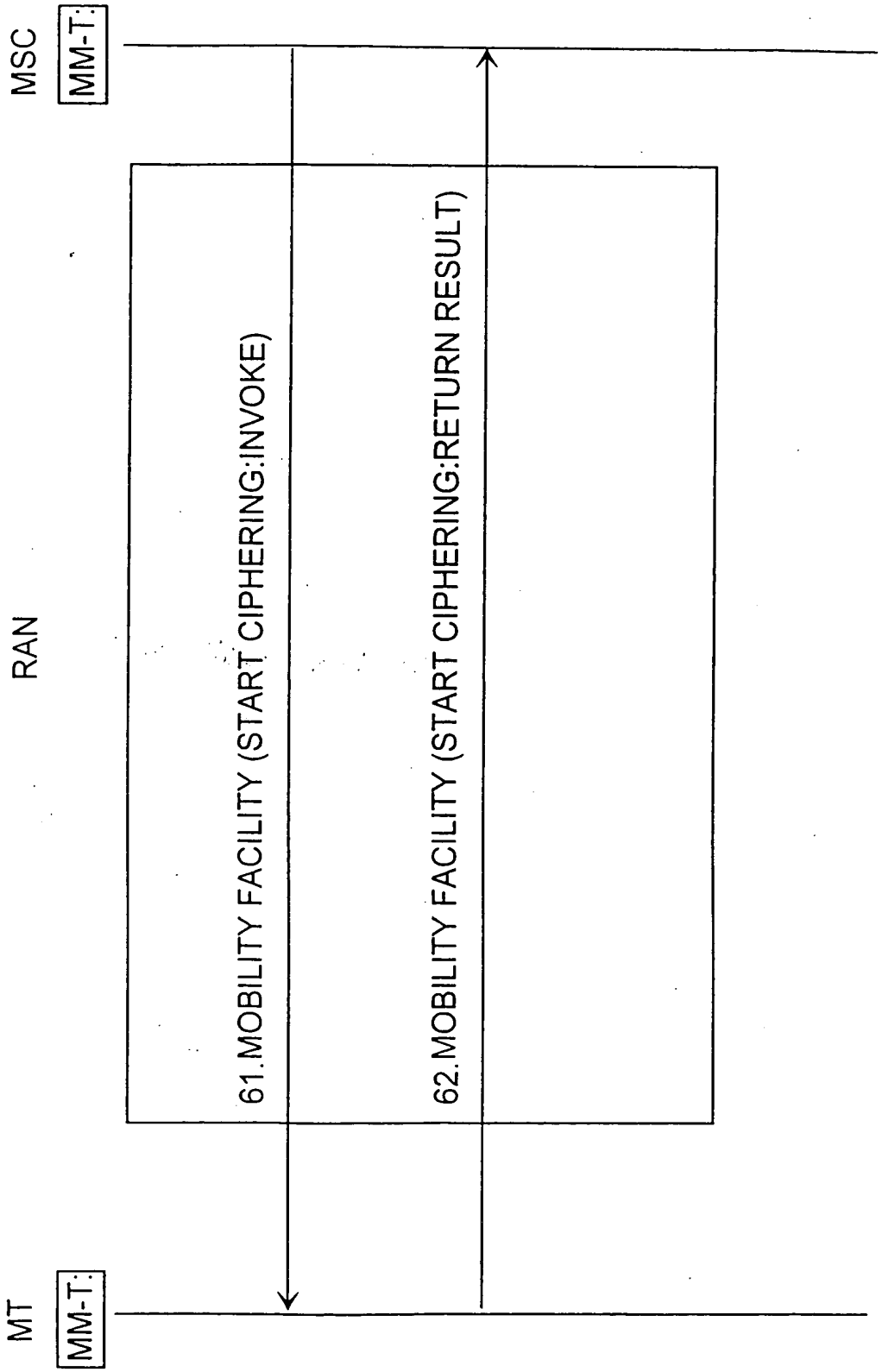
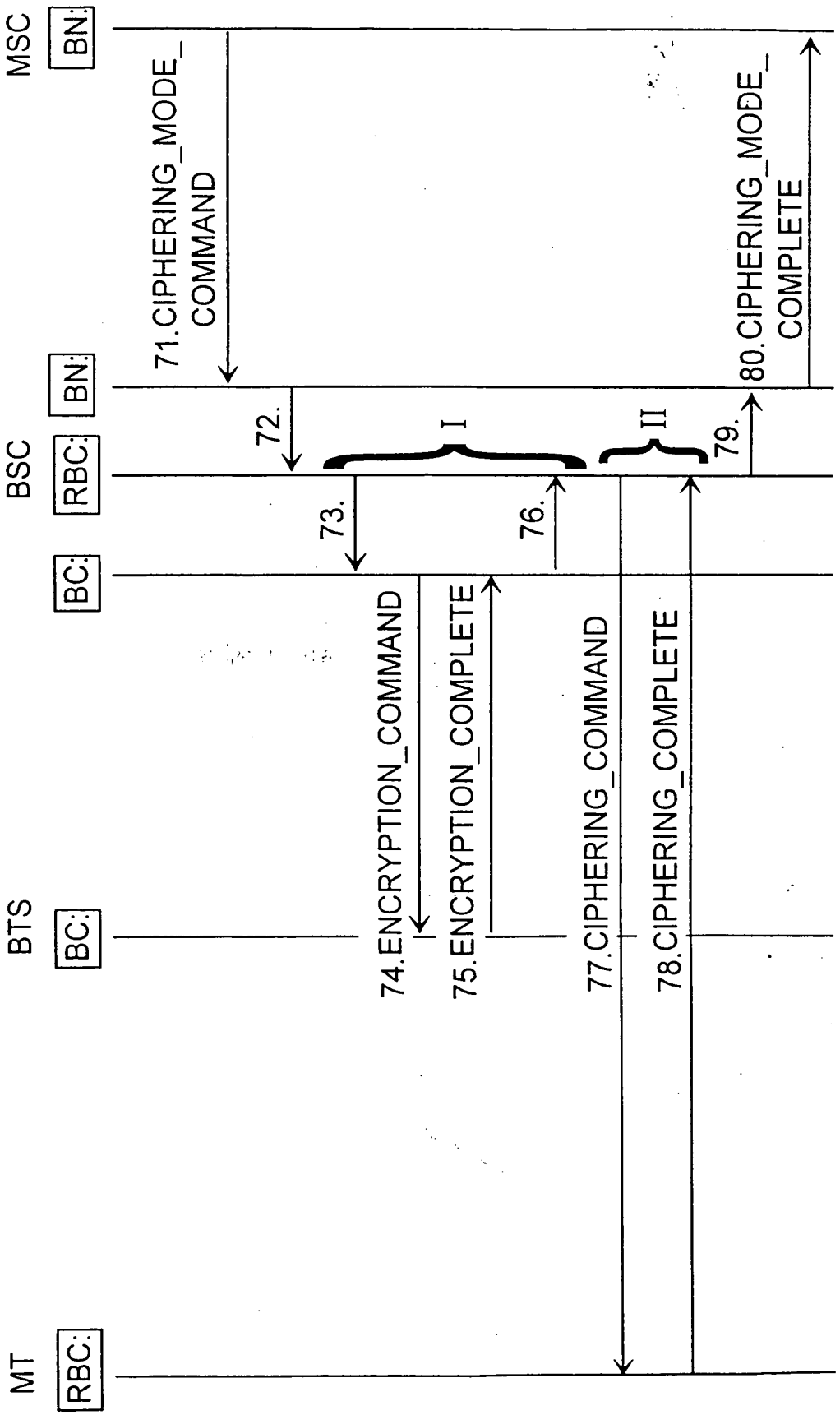

MSC
MM-T:
RAN
61.MOBILITY FACILITY (START CIPHERING:INVOKE)
62.MOBILITY FACILITY (START CIPHERING:RETURN RESULT)
MT
MM-T:

Fig. 7


MSC
BN:
BSC
RBC:
BN:
BC:
BTS
BC:
MT
RBC:
71.CIPHERING_MODE_ COMMAND
72.
73.
74.ENCRYPTION_COMMAND
75.ENCRYPTION_COMPLETE
76.
77.CIPHERING_COMMAND
78.CIPHERING_COMPLETE
79.
80.CIPHERING_MODE_ COMPLETE
I
II